2次体のmod $\mathfrak{p}$のray class fieldの2次部分拡大について (代数的整数論とその周辺)

AUTHOR(S):

河本, 史紀

CITATION:

河本, 史紀. 2次体のmod $\mathfrak{p}$のray class fieldの2次部分拡大について (代数的整数論とその周辺). 数理解析研究所講究録 1999, 1097: 69-81

ISSUE DATE:

1999-04

URL:

http://hdl.handle.net/2433/63021

数理解析研究所講究録
1097 巻 1999 年 69-81

2 次体の mod $\mathfrak{p}$ の ray class field の 2 次部分拡大について

学習院大学理学部　河本 史紀　(Fuminori Kawamoto)

1. Introduction

F を有限次代数体とし，$\mathfrak{o}_F$ で F の整数環を表わす．K/F を有限次 Galois 拡大とし，$G := Gal(K/F)$ をこの拡大の Galois 群とする．そのとき，$\alpha \in \mathfrak{o}_K$ が存在して，$\{s(\alpha)\}_{s\in G}$ が $\mathfrak{o}_K$ の free $\mathfrak{o}_F$–basis になるならば，この Galois 拡大 K/F は normal integral basis (**以下 NIB と略す**) をもつという．さらに，このような α を K/F の NIB の生成元と呼ぶことにする．

この講演では最近得た NIB の存在に関する結果 [13] の紹介をすることが目的である．まず，次のことはよく使うので注意していただきたい．

注意 1.　M は K/F の中間体で，M/F は Galois 拡大であると仮定する．このとき，K/F が NIB をもち，$\alpha \in \mathfrak{o}_K$ が K/F の NIB の生成元ならば，$Tr_{K/M}(\alpha)$ は M/F の NIB の生成元になる．したがって，M は F 上 NIB をもたなければ K も F 上 NIB をもたない．□

次に，NIB の存在に関する問題の歴史と知られている結果について簡単に記す．そもそも，NIB ということばを初めて定義し，最初の結果を与えたのは，Hilbert (1897) であった (ただし，彼は NIB を Normalbasis と呼んでいる ([9, §105 (p.216); cf. §3])):

定理 2 (Hilbert). ([9, Satz 132])　$F := \mathbb{Q}$ とし，$K/\mathbb{Q}$ を n 次 Abel 拡大とする．このとき，n と $K/\mathbb{Q}$ の判別式が素ならば $K/\mathbb{Q}$ は NIB をもつ．

仮定の条件から $K/\mathbb{Q}$ は tamely ramified であることがわかる．一般に，Galois 拡大 K/F が NIB をもつならば tamely ramified でなければならない (cf. [10, Theorem 1.3])．その後上の定理は，$K/\mathbb{Q}$ が NIB をもつ必要十分条件はこの拡大が tamely ramified であること，へ拡張される (Hilbert–Speiser の定理)．さて，Kummer は円の素数分体に対する Stickelberger の定理を証明したが，Hilbert は定理 2 を使ってこの結果の証明を与えている ([9, Satz 136 とその直後]; しかしながら，Satz 89 の証明には軽い欠点がある (Washington [15, Remarks, (2)]))．なお，この Hilbert の方針に従う，任意の円分体に対する Stickelberger の定理の証明は，Fröhlich [4] にある．$\mathbb{Q}$ 上の，Abel とは限らない Galois 拡大に関しては，Taylor の定理 (1981) から導かれる次の結果がある．

定理 3 (Taylor). (Cf. [10, Theorem 2.1])　$F := \mathbb{Q}$ とし，$K/\mathbb{Q}$ を奇数次数の tamely ramified Galois 拡大とする．このとき，$K/\mathbb{Q}$ は NIB をもつ．

基礎体 F が $\mathbb{Q}$ と異なる場合，いくつかの結果があるが，詳しくは [10] を参照されたい．ここでは，Brinkhuis による不分岐 Abel 拡大 K/F に関する次の結果のみ引用する．

定理 4 (Brinkhuis). ([1, Corollary 2.10] または [2, Corollary 2.1]) F を総実代数体とし，K/F を F のすべての有限素点が不分岐な Abel 拡大とする．このとき，$Gal(K/F)$ が $(2, \cdots, 2)$ 型でないならば，K/F は NIB をもたない．

この定理は後で使う (定理 13)．我々は次のような拡大の NIB を問題にすることにする．F の整因子 $\mathfrak{m}$ に対して，$F(\mathfrak{m})$ で F の mod $\mathfrak{m}$ の the ray class field を表わす．とくに，$F(1)$ は F の Hilbert 類体であり，$h_F := [F(1) : F]$ とおく．

問題 5. $\mathfrak{m}$ が平方因子をもたないとき，tamely ramified Abel 拡大 $F(\mathfrak{m})/F$ は normal integral basis をもつのか．もしそうならば，その生成元を決めよ．□

$\mathfrak{m}$ が平方因子をもたないときに限り，$F(\mathfrak{m})/F$ は tamely ramified になるから，この仮定は必要である．$F = \mathbb{Q}$ のときは $F(\mathfrak{m})$ は円分体か，またはその最大実部分体になるから，$F(\mathfrak{m})/F$ は NIB をもつ．さらに，$F \subset k \subsetneq K \subset F(\mathfrak{m})$ としたとき，K/k の NIB の存在も気になる．[11, Theorem 5.3] では，$F = \mathbb{Q}$ かつ $\mathfrak{m} = p\infty$ のとき K/k の NIB の存在を調べた (p は奇素数で，∞ は $\mathbb{Q}$ の唯一つの無限素点である)．その結論として，拡大次数が 2 ベキのものを除くと，多くの K/k は NIB をもたないことが得られた．では，一般の F についてはどうなるのであろうか．そこで F が 2 次体のとき問題 5 を考えることにする．F を 2 次体にする理由は，体次数が小さいので単数群のランクも小さく，問題が扱いやすいからである．得られた結果は，$F = \mathbb{Q}$ の場合とは大分違うものになり，面白かった．ところで，$F(\mathfrak{m})/F$ が relative integral basis (RIB **と略す**) をもつのか気になるだろう．もしそうでないならば，NIB をもちはしないのだから．これに関して次が成り立つ．

命題 6. F を有限次代数体とし，$\mathfrak{m}$ を平方因子をもたない F の整因子とする．F の類数 h_F は奇数であると仮定する．このとき，$F(\mathfrak{m})/F$ は RIB をもつ．

証明. $K := F(\mathfrak{m})$, $n := [K : F]$ とおく．$\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ を $\mathfrak{m}$ の有限部分 $\mathfrak{m}_0$ のすべての素因子とする．$1 \leq \forall i \leq s$ に対して，e_i, f_i, g_i を各々 $\mathfrak{p}_i$ の K/F における分岐指数, 相対次数, 分解の個数とする．また，$\mathfrak{P}_i$ を $\mathfrak{p}_i$ の上にある $\mathfrak{o}_K$ の素イデアルとし，これを 1 つとり固定する．$D_{K/F}$ で K/F の差積を表わし，Z_i を $\mathfrak{p}_i$ の K/F における分解群とする．$\forall \sigma \in Z_i$ について，$\mathfrak{P}_i^\sigma$ は K/F において tamely ramified であるから，$\mathrm{ord}_{\mathfrak{P}_i^\sigma}(D_{K/F}) = e_i - 1$ である．したがって，

$$D_{K/F} = \prod_{i=1}^{s} \prod_{\sigma \in Z_i} \mathfrak{P}_i^{(e_i-1)\sigma}.$$

$d_{K/F}$ で K/F の判別式を表わすと，$N_{K/F}\mathfrak{P}_i^\sigma = N_{K/F}\mathfrak{P}_i = \mathfrak{p}_i^{f_i}$ より，

$$d_{K/F} = N_{K/F}D_{K/F} = \prod_{i=1}^{s} \prod_{\sigma \in Z_i} \mathfrak{p}_i^{(e_i-1)f_i} = \prod_{i=1}^{s} \mathfrak{p}_i^{(e_i-1)f_i g_i}. \tag{1}$$

各 i $(1 \leq i \leq s)$ について,

$$e_i f_i g_i = n = [K : F(\mathfrak{m}\mathfrak{p}_i^{-1})][F(\mathfrak{m}\mathfrak{p}_i^{-1}) : F(1)]h_F.$$

$\mathfrak{m}$ は平方因子をもたないから, $\mathfrak{p}_i \nmid \mathfrak{m}\mathfrak{p}_i^{-1}$. よって, $\mathfrak{p}_i$ は $F(\mathfrak{m}\mathfrak{p}_i^{-1})/F$ において不分岐である. ゆえに, $e_i \mid [K : F(\mathfrak{m}\mathfrak{p}_i^{-1})]$ を得る. したがって, 上式から $h_F \mid f_i g_i$. (1) より $d_{K/F}$ は単項イデアルである. ところで, Artin の結果によれば, θ を有限次拡大 K/F の任意の原始元 $(K = F(\theta))$ とすると, $\mathfrak{o}_F$ の分数イデアル $\mathfrak{a}$ が存在して, $d_{K/F} = d_{K/F}(1, \theta, \theta^2, \cdots, \theta^{n-1})\mathfrak{a}^2$ と書ける. ここで, $d_{K/F}(1, \theta, \theta^2, \cdots, \theta^{n-1})$ は $1, \theta, \theta^2, \cdots, \theta^{n-1}$ の K/F における判別式を表わす. さらに, K/F が RIB をもつ必要十分条件は $\mathfrak{a}$ が単項イデアルになることである ([3, 第 3 章, 定理 4.9 系 2 と定理 4.10] にそれらの詳しい説明がある). 上に述べたことから, $\mathfrak{a}^2$ は単項であり, h_F は奇数だから $\mathfrak{a}$ が単項イデアルになる. ゆえに, K/F は RIB をもつ. □

2. 使う方法と準備 (体 $K^{\mathfrak{p}}$ の定義)

我々は F が 2 次体のときに問題 5 を扱う. F が $h_F > 1$ をみたす実 2 次体のときは, 定理 13 より $F(\mathfrak{m})/F$ は 'ほとんど' NIB をもたないことがわかる. したがって, $h_F = 1$ のときに問題 5 の答えを見つけなければならない. また, F が偶数類数をもつ虚 2 次体の場合には, 命題 34 から $F(\mathfrak{m})/F$ は NIB をもたない. よって, 奇数類数のときに問題 5 を扱うことになる. そして, 注意 1 を考慮すれば $\mathfrak{m}$ が素イデアルのときをまず初めに考えるべきであろう. そこで次のような体を考える.

定義 7. (体 $K^{\mathfrak{p}}$ の定義) F を奇数類数をもつ有限次代数体とし, $\mathfrak{p}$ をある奇素数の上にある $\mathfrak{o}_F$ の素イデアルとする. $a_{\mathfrak{p}} := [F(\mathfrak{p}) : F(1)]$ とおき, $a_{\mathfrak{p}}$ は偶数であると仮定する. このとき, $F(\mathfrak{p})/F$ の 2 次部分拡大 K/F が一意的に存在する. なぜなら, $F(\mathfrak{p})/F(1)$ は偶数次巡回拡大だから, その 2 次部分拡大 $M/F(1)$ が一意的に存在する. そして, M/F は Abel 拡大で, $F(1)/F$ は奇数次拡大であるから, M/F の 2 次部分拡大 K/F が一意的に存在することがわかる. そこで, $\mathfrak{p}$ により一意的に決まるこの体 K を $K^{\mathfrak{p}}$ と書くことにする. $\mathfrak{p} \nmid 2$ より $K^{\mathfrak{p}}/F$ は tamely ramified であり, $\mathfrak{p}$ のみが分岐する分岐拡大である. □

もし $K^{\mathfrak{p}}/F$ が NIB をもたないならば, 注意 1 により $F(\mathfrak{p})/F$ も NIB をもたないことがわかる. また, $[F(\mathfrak{p}) : F] = 2$ かつ $K^{\mathfrak{p}}/F$ が NIB をもつならば, $F(\mathfrak{p})/F$ は NIB をもつこともわかる. このように $\mathfrak{m} = \mathfrak{p}$ に関する問題 5 の答えを見つけられる (でも, 完全解答ではありません). これらに対する具体例については, 注意 19 および例 21, 22, 24, 27, 28, 29, 30, 31, 32 を参照せよ.

注意 8. 密度定理により, $a_{\mathfrak{p}}$ は偶数であり, $K^{\mathfrak{p}}/F$ は NIB をもち, かつ $\mathfrak{p}$ が $F/\mathbb{Q}$ で完全分解するような $\mathfrak{o}_F$ の素イデアル $\mathfrak{p}$ は無限個存在することがわかる. □

注意 9. Gómez Ayala and Schertz [7, Satz 1] は次のことを示している: $F = \mathbb{Q}(\sqrt{m})$, $m = -2, -11, -19, -43, -67, -163$ $(h_F = 1)$ のとき, $K^{\mathfrak{p}}/F$ が, したがって $F(\mathfrak{p})/F$ が NIB をもたないような $\mathfrak{o}_F$ の素イデアル $\mathfrak{p}$ が無限個存在する. 上の方法は彼らの方法の一般化であり, F が虚 2 次体のとき我々はこの結果の拡張を得ることができる (定理 37 と注意 38 を参照のこと). □

F の単項イデアルからなる群を考える:

$$S_4 := \{\, x\mathfrak{o}_F \mid x \in F^\times,\ x \equiv 1 \mod 4 \text{ かつ } x \text{ は総正} \,\}.$$

$K^{\mathfrak{p}}/F$ は 2 次拡大だから, NIB の存在に関する判定条件は次のように簡潔に書ける.

命題 10. 定義 7 と同じ仮定の下で, $K^{\mathfrak{p}}/F$ が NIB をもつ必要十分条件は, $\mathfrak{p} \in S_4$ である. さらに $\mathfrak{p} = \pi\mathfrak{o}_F$, $\pi \in \mathfrak{o}_F$, $\pi \equiv 1 \mod 4$ かつ π は総正ならば, $\{(1+\sqrt{\pi})/2, (1-\sqrt{\pi})/2\}$ は $\mathfrak{o}_{K^{\mathfrak{p}}}$ の free $\mathfrak{o}_F$–basis になる.

注意 11. 以下に述べるすべての結果において $\mathfrak{p} \in S_4$ が成り立つとき, $\mathfrak{p}$ の生成元 π を具体的に決定している. $a_{\mathfrak{p}}$ が偶数であるという仮定は, 必ずしも強い条件とはならない. 実際, F があるタイプの奇数類数の実 2 次体か, または奇数類数の虚 2 次体のとき, $\mathfrak{p}$ が $F/\mathbb{Q}$ で惰性するならば $a_{\mathfrak{p}}$ は偶数になる (定理 18 と命題 36 を参照のこと). □

論文 [13] を書くことになるきっかけは, Gómez Ayala and Schertz [7] にあった. 小松 啓一さんからこの論文に関連する質問をされた: F が実 2 次体で, $[F(\mathfrak{p}) : F] = 2$ のとき, $F(\mathfrak{p})/F$ が NIB をもつ, またもたないような $\mathfrak{p}$ の例はあるかと聞かれたと思う (答えはどちらもあります; それらが無限個あるかどうかは示せなかったが). それで [7] の結果を分析するために, ドイツ語を小松さんに教えていただきながら自家製ノートを作り始めたのが 1996 年 2 月 25 日である. 具体例が知りたくて, 計算機でプログラムを書くことにする. ぼくにとってこれはほぼ初めての経験だった. UBASIC (木田ソフト) を使うことにする. 呼び出し関数として 2 次体の類数と基本単数が求められ, とても便利だった. 素イデアル $\mathfrak{p}$ が単項であるか否かを判定し, そうならばその生成元を求めるための計算方法が知りたくて文献を漁ったが, 結局, 高木の初等整数論講義が役に立ったのには驚いた. 明示的には書かれていないのだが, よく読むとヒントになることが散りばめられていた. 和田 秀男さんがよく, "高木の初等整数論講義は面白い本ですね" とおっしゃっていた意味がわかったような気がした. プログラムを動かしてデータをとると, いくつかのパターンが顕れる. それほど複雑なことを扱っているわけではないので, これは一般に成り立つだろうと確信できた. 小松さんの御厚意により, 1997 年 3 月の早稲田大学におけるシンポジウムにおいて, このことを予想として話させていただいた. 計算機は予想を教えてくれたが, 残念ながらその証明を教えてくれなかった. 奇素数および 4 を法とした, 実 2 次体の基本単数の位数およびその挙動をどう捕らえたらよいかわからなかった. 幸いにも, ぼくの講演を聴いていた Lemmermeyer さんがそのヒントを与えてくださった (cf. [12]). それで予想の証明方法が, 順々にわかってきた. その過程において, 計算機は証明を教

えてくれなかったけど, 証明を推し進める上で力強い支援をしてくれることがわかった. こうしてここで述べる結果を得ることになったのである. ぼくにとって初めての経験が多くて, とても面白かった.

そういう理由で, 小松さんと Lemmermeyer さんの御厚意には心から感謝いたします. また, この原稿を書く上で, 市村 文男さんから助言をいただきました. とくに, 命題 6 を考えることを強く勧められました. お三人の方, 本当にありがとうございました.

注意 12. 1999 年 1 月末, 文献 [6] と [8] の存在を知りました. それで, [13] の内容を書き換えています. Section 4 の F が虚 2 次体の場合の結果が大幅によくなりそうなのですが, この原稿は元のままにしておきます. とくに, ここで述べた方法が $F(\mathfrak{p})/F(1)$ の NIB の非存在に関する結果を出すのに使えそうです. □

3. 実 2 次体に関する結果

この節において, $F=\mathbb{Q}(\sqrt{m})$ を実 2 次体とする. だだし, $m\in\mathbb{Z}$ は $m>1$ をみたし, 平方因子をもたない. $\varepsilon\,(>1)$ を F の基本単数とする.

F の類数が 1 でないときは, 定理 4 と F の単数群のランクが 1 であることから次のことがわかる.

定理 13. g を既約剰余類群 $(\mathfrak{o}_F/4\mathfrak{o}_F)^\times$ における $\varepsilon \bmod 4$ の位数とする. $h_F>1$ と仮定する. このとき, $F(1)/F$ が NIB をもつための必要十分条件は, $h_F=2$ かつ g が奇数であり, さらにこれが成り立つとき, $\{(1+\sqrt{\varepsilon^g})/2,\ (1-\sqrt{\varepsilon^g})/2\}$ は $\mathfrak{o}_{F(1)}$ の free $\mathfrak{o}_F$–basis になる. とくに, $h_F\neq 2$ または g が偶数ならば, F の任意の (平方因子をもたない) 整因子 $\mathfrak{m}$ について $F(\mathfrak{m})/F$ は NIB をもたない.

注意 14. $(\mathfrak{o}_F/4\mathfrak{o}_F)^\times$ の平方元の計算により, $g\mid 2,\ 4$ または 6 を得る (cf. [14, Proposition 1 の証明]). したがって, g が奇数ならば $g=1$ または 3. $m=39,\ 55,\ 66,\ 105,\ 114,\ 146,\ 155,\ 178,\ 203$ のとき, $h_F=2$ かつ $g=1$. $m=205,\ 221$ のときは, $h_F=2$ かつ $g=3$. □

定理 13 は, 問題 5 の解答としてほぼ満足できるものである. 次に, 類数が 1 の実 2 次体を扱わなければならない. 以下に述べるほとんどの結果は, 類数が 1 に限らず, 奇数類数をもつ実 2 次体に対して成り立つ. そこで, **いまから h_F は奇数であると仮定する**. そのとき, genus theory により m の形は次のようになる:

$$
\begin{array}{lllll}
\text{Case 1} & m=\ell, & \ell\text{: 素数}, & \ell\equiv 3 \bmod 4, & \\
\text{Case 2} & m=\ell_1\ell_2, & \ell_1\text{: 素数}, & \ell_1\equiv 3 \bmod 4, & \ell_2:=2,\\
\text{Case 3} & m=\ell_1\ell_2, & \ell_i\text{: 素数}, & \ell_i\equiv 3 \bmod 4 & (i=1,\ 2),\\
\text{Case 4} & m=\ell, & \ell\text{: 素数}, & \ell\equiv 1 \bmod 4, &
\end{array}
$$

または $m=2$ ([5, Corollary of Theorem 2.17]). 初めの 3 つの場合では, $N_{F/\mathbb{Q}}\varepsilon=1$ であり, 後の 2 つの場合は $N_{F/\mathbb{Q}}\varepsilon=-1$ であることを注意する.

以下, この節の最後まで $\mathfrak{p}$ を奇素数 p の上にある $\mathfrak{o}_F$ の素イデアルとする.

命題 10 を使って得られる結果は, $\mathfrak{p}$ の $F/\mathbb{Q}$ における分岐の仕方により異なる. $\mathfrak{p}$ が分岐, 惰性, 分解する順にそれらを述べてゆく.

定理 15. $\mathfrak{p}$ は $F/\mathbb{Q}$ で分岐すると仮定する. $F=\mathbb{Q}(\sqrt{m})$ は Case 4 の奇数類数の実 2 次体であり, かつ $m\equiv 1 \mod 8$ をみたすとする (これら 2 つの仮定をみたさなければ, $2\nmid a_{\mathfrak{p}}$ となる). このとき, $2\mid a_{\mathfrak{p}}$ かつ $K^{\mathfrak{p}}/F$ は NIB をもつ.

次の定理は, $F(\mathfrak{p})/F$ の奇素数次部分拡大についての考察 [11, Proposition 4.5] を使って示せる.

定理 16. $F=\mathbb{Q}(\sqrt{m})$ を類数 1 の実 2 次体とする. $\mathfrak{p}$ は $F/\mathbb{Q}$ で分岐すると仮定する. Case $1\sim 3$ において $p\neq 3$, Case 4 においては $p-1$ が 2 ベキではない ($p\neq 5$ かつ $p\equiv 5 \mod 8$ ならば $p-1$ は 2 ベキではない) と仮定する. このとき, $F(\mathfrak{p})/F$ は NIB をもたない.

例 17. $m=p=41$ とする. そのとき, F は Case 4 の体であり, $h_F=1$, $[F(\mathfrak{p}):F]=(p-1)/4=10$. 定理 15 より $K^{\mathfrak{p}}/F$ は NIB をもつが, 定理 16 より $F(\mathfrak{p})/F$ は NIB をもたない. □

定理 18. $\mathfrak{p}$ は $F/\mathbb{Q}$ で惰性すると仮定する. また, $2\mid a_{\mathfrak{p}}$ と仮定する (この条件は, $N_{F/\mathbb{Q}}\varepsilon=1$ または "$N_{F/\mathbb{Q}}\varepsilon=-1$ かつ $p\equiv 1 \mod 4$" のときに限り成り立つことがわかる). このとき, $m\equiv 2 \mod 4$ かつ $\varepsilon\equiv 1+2\sqrt{m} \mod 4$ ならば, $K^{\mathfrak{p}}/F$ が NIB をもつ $\Longleftrightarrow p\equiv 1 \mod 4$. その他のときは $K^{\mathfrak{p}}/F$ はいつも NIB をもつ.

注意 19. F を Case 2 の体とする. $\delta:=1$ または 3 とおく. このとき, 密度定理により $p\equiv\delta \mod 4$ をみたし, かつ $F/\mathbb{Q}$ で惰性する奇素数 p は無限個ある. したがって, $m\equiv 2 \mod 4$ かつ $\varepsilon\equiv 1+2\sqrt{m} \mod 4$ ならば (例えば $m=6, 22, 38, 86, 118, \cdots$ のとき), $K^{\mathfrak{p}}/F$ が NIB をもつような惰性する素イデアル $\mathfrak{p}$ は無限個あるし, そうでないものも無限個存在する. □

いまからこの節の最後まで, $\mathfrak{p}$ は単項イデアルであり, $F/\mathbb{Q}$ において完全分解すると仮定する.

$\mathfrak{p}=\pi\mathfrak{o}_F$ かつ $\pi>0$ をみたす $\pi\in\mathfrak{o}_F$ を 1 つとり固定する. π の $F/\mathbb{Q}$ における非自明な共役を π' で表わす. $\pi=a+b\omega$ ($a,\ b\in\mathbb{Z}$) とかく. ここで, $m\not\equiv 1$ (resp. $m\equiv 1$) $\mod 4$ ならば $\omega:=\sqrt{m}$ (resp. $:=(1+\sqrt{m})/2$) とおいた. また, $m\equiv 1 \mod 4$ ならば $M:=(m-1)/4$ とおく.

定理 20. $F=\mathbb{Q}(\sqrt{m})$ を Case 1 または 2 の体とする. $2\mid a_{\mathfrak{p}}$ と仮定する (この条件は, $p\equiv 1 \mod 8$ と同値になる). このとき,

(I) Case 1 では, $K^{\mathfrak{p}}/F$ は NIB をもつ.

(II) Case 2 では, a は奇数であり, ε が mod 4 で次の 2 つのいずれかに合同になり, 各主張が成り立つ.

(i) $\varepsilon \equiv -1 \mod 4$ ならば, $p \equiv 1$ (resp. $\equiv 9$) mod 16 のとき, $K^{\mathfrak{p}}/F$ は NIB をもつ $\Longleftrightarrow a \equiv \pm 1$ (resp. $\equiv \pm 3$) mod 8.

(ii) $\varepsilon \equiv 1 + 2\sqrt{m} \mod 4$ ならば, $K^{\mathfrak{p}}/F$ は NIB をもつ $\Longleftrightarrow a \equiv 1$ mod 4.

例 21 (Case 2; (II–i)). $m = 2 \cdot 7$ のとき, $h_F = 1$, $\varepsilon = 15 + 4\sqrt{m} \equiv -1 \mod 4$.

p	p mod 16	$a_{\mathfrak{p}}$	π	a mod 8
1009	1	2	$153 - 40\sqrt{m}$	1
193	1	2	$47 - 12\sqrt{m}$	-1
113	1	2	$83 - 22\sqrt{m}$	3
449	1	56	$85 - 22\sqrt{m}$	-3
617	9	2	$659 - 176\sqrt{m}$	3
137	9	4	$61 - 16\sqrt{m}$	-3
457	9	2	$801 - 214\sqrt{m}$	1
233	9	4	$143 - 38\sqrt{m}$	-1

例 22 (Case 2; (II–ii)). $m = 2 \cdot 3$ のとき, $h_F = 1$, $\varepsilon = 5 + 2\sqrt{m} \equiv 1 + 2\sqrt{m}$ mod 4.

p	$a_{\mathfrak{p}}$	π	a mod 4
73	2	$113 - 46\sqrt{m}$	1
97	8	$79 - 32\sqrt{m}$	3

定理 23. $F = \mathbb{Q}(\sqrt{m})$ を Case 3 の体とする. $2 \mid a_{\mathfrak{p}}$ と仮定する (この条件は, ℓ_1 が mod p で平方剰余であることと, あるいは $\pi' > 0$ と同値になる). このとき, ε は mod 4 で次の 3 つのいずれかに合同になり, 各主張が成り立つ.

(i) $\varepsilon \equiv -1 \mod 4$ のとき, $m \equiv 1 \mod 8$ ならば $K^{\mathfrak{p}}/F$ は NIB をもつ. $m \equiv 5 \mod 8$ ならば, $K^{\mathfrak{p}}/F$ が NIB をもつための必要十分条件は b が偶数になることである.

(ii) $\varepsilon \equiv M + 1 + \omega$ または $-(M + \omega) \mod 4$ のとき, $K^{\mathfrak{p}}/F$ は NIB をもつ.

例 24 (Case 3; (i)). $m = 3 \cdot 47 = 141 \equiv 5 \mod 8$ のとき, $h_F = 1$, $\varepsilon = 87 + 16\omega \equiv -1 \mod 4$.

p	$a_\mathfrak{p}$	π	$\pi \bmod 4$
61	2	$129 - 20\omega$	1
397	2	$5639 - 876\omega$	-1
37	2	$264 - 41\omega$	3ω
97	6	$573 - 89\omega$	$1 + 3\omega$
157	6	$72 - 11\omega$	ω
601	2	$7023 - 1091\omega$	$3 + \omega$

定理 25. $F = \mathbb{Q}(\sqrt{m})$ を Case 4 の体とする. $2 \mid a_\mathfrak{p}$ と仮定する. このとき, ε は mod 4 で次の 3 つのいずれかに合同になり, 各主張が成り立つ.

(i) $\varepsilon \equiv (1-2M)\sqrt{m} \mod 4$ のとき, $K^\mathfrak{p}/F$ が NIB をもつ $\Longleftrightarrow \pi \equiv 1$ または $(1-2M)\sqrt{m} \mod 4$.

(ii) $\varepsilon \equiv M-1+\omega$ または $M-2+\omega \mod 4$ のとき, $m \equiv 5 \mod 8$ であり, かつ $K^\mathfrak{p}/F$ が NIB をもつ $\Longleftrightarrow \pi \equiv 1$, $M+\omega$, $-(M+1+\omega)$, $1+2\omega$, $M-2+\omega$ または $M-1+\omega \mod 4$.

注意 26. 計算機を使って $a_\mathfrak{p}$ を求めることはできる. しかしながら, 定理 20, 23 のように $a_\mathfrak{p}$ が偶数になるための特徴付けをこの Case では見つけることができなかった. それ故 Case 4 の体の手強さを感じた. □

例 27 (Case 4; (i)). $m = 409 \equiv 1 \mod 8$ のとき, $h_F = 1$, $\varepsilon = 106387620283 + 11068353370\omega \equiv 3 + 2\omega \equiv \sqrt{m} \mod 4$.

p	$a_\mathfrak{p}$	π	$\pi \bmod 4$
17	4	$85 - 8\omega$	1
101	2	$-74177 + 6990\omega$	$3 + 2\omega$
2333	2	$12150526462405 - 1144993450182\omega$	$1 + 2\omega$

例 28 (Case 4; (i)). $m = 37 \equiv 5 \mod 8$ のとき, $h_F = 1$, $\varepsilon = 5 + 2\omega \equiv 1 + 2\omega \equiv -\sqrt{m} \mod 4$.

p	$a_\mathfrak{p}$	π	$\pi \bmod 4$
269	2	$185 - 52\omega$	1
877	6	$-587 + 166\omega$	$1 + 2\omega$
149	2	$-29 + 9\omega$	$3 + \omega$
157	2	$-44 + 13\omega$	ω
229	2	$118 - 33\omega$	$2 + 3\omega$
593	2	$281 - 79\omega$	$1 + \omega$

例 29 (Case 4; (ii)). $m = 2293 \equiv 5 \mod 16$ のとき, $h_F = 1$, $\varepsilon = 21890901812 + 933807029\omega \equiv \omega \mod 4$.

p	$a_\mathfrak{p}$	π	$\pi \bmod 4$
37	2	$22585 - 924\omega$	1
61	6	$27797221 - 1137243\omega$	$1 + \omega$
193	2	$101401959638 - 4148568261\omega$	$2 - \omega$
541	2	$-83814171383 + 3429014710\omega$	$1 + 2\omega$
17	2	$-1665937 + 68157\omega$	$-1 + \omega$
709	2	$-16081478656 + 657927245\omega$	ω
6397	6	$4093107546520 - 167457671597\omega$	3ω
8681	4	$9233533239433 - 377763339789\omega$	$1 + 3\omega$
12401	8	$6464258805691 - 264466475874\omega$	$3 + 2\omega$

例 30 (Case 4; (ii)). $m = 2749 \equiv 13 \mod 16$ のとき, $h_F = 1$, $\varepsilon = 57581648522 + 2239184645\omega \equiv 2 + \omega \mod 4$.

p	$a_{\mathfrak{p}}$	π	$\pi \bmod 4$
73	2	$9200161 - 344376\omega$	1
53	2	$5203075 - 194759\omega$	$3 + \omega$
149	2	$668 - 25\omega$	$-\omega$
317	2	$-14782355 + 553326\omega$	$1 + 2\omega$
401	4	$-111163 + 4161\omega$	$1 + \omega$
37	2	$-26 + \omega$	$2 + \omega$
2393	2	$1751825973070 - 65573506953\omega$	$2 + 3\omega$
641	2	$15827232566287 - 592437354330\omega$	$3 + 2\omega$
2797	2	$37901608992655 - 1418714791889\omega$	$3 + 3\omega$

例 31 (Case 4; (ii)). $m = 1621 \equiv 5 \mod 16$ のとき, $h_F = 1$, $\varepsilon = 2351907622159 + 119806883557\omega \equiv -1 + \omega \mod 4$.

p	$a_{\mathfrak{p}}$	π	$\pi \bmod 4$
37	2	$1733 - 84\omega$	1
617	28	$525235789 - 25458791\omega$	$1 + \omega$
5	2	$7084810 - 343409\omega$	$2 - \omega$
277	2	$-1279 + 62\omega$	$1 + 2\omega$
853	6	$-29729 + 1441\omega$	$-1 + \omega$
293	2	$-1985696 + 96249\omega$	ω
1049	4	$2011213196644 - 97485848265\omega$	3ω
2053	18	$37341509901229 - 1809986516741\omega$	$1 + 3\omega$
1301	26	$939543590279 - 45540773118\omega$	$3 + 2\omega$

例 32 (Case 4; (ii)). $m = 1549 \equiv 13 \mod 16$ のとき, $h_F = 1$, $\varepsilon = 329861957297 + 17199418961\omega \equiv 1 + \omega \mod 4$.

p	$a_{\mathfrak{p}}$	π	$\pi \bmod 4$
5	2	$10910929 - 540716\omega$	1
269	2	$280489447 - 13900295\omega$	$3 + \omega$
461	2	$786913696 - 38997305\omega$	$-\omega$
97	2	$-4521515 + 224074\omega$	$1 + 2\omega$
41	4	$-13483003 + 668181\omega$	$1 + \omega$
181	6	$-2038 + 101\omega$	$2 + \omega$
1373	2	$57513163038590 - 2850196116717\omega$	$2 + 3\omega$
853	2	$830164603987 - 41140702502\omega$	$3 + 2\omega$
7757	2	$8936594235931 - 442873332681\omega$	$3 + 3\omega$

注意 33. $m = 2$ かつ $2 \mid a_{\mathfrak{p}}$ と仮定する. そのとき, いつも $K^{\mathfrak{p}}/F$ は NIB をもつように思えるが, 証明はできなかった. □

4. 虚 2 次体に関する結果

この節において, $F = \mathbb{Q}(\sqrt{m})$ を虚 2 次体とする. だだし, $m \in \mathbb{Z}$ は $m < 0$ をみたし, 平方因子をもたない.

命題 34. F を偶数類数をもつ虚 2 次体とする. このとき, $F(1)/F$ は NIB をもたない. とくに, F の任意の (平方因子をもたない) 整因子 $\mathfrak{m}$ について $F(\mathfrak{m})/F$ は NIB をもたない.

命題 34 は, 問題 5 の解答となる. 次に, h_F は奇数であると仮定し, 命題 10 を使って問題 5 に取り組む. ところが, 分岐する $\mathfrak{o}_F$ の素イデアルには命題 10 を適用することはできないことを注意する. いま, h_F は奇数であるから genus theory より $m = -1$, -2 または $-\ell$ となる. ただし, ℓ は $\ell \equiv 3 \mod 4$ をみたす素数である.

命題 35. $m := -1$ または -3 とする. $\mathfrak{p}$ を奇素数 p の上の $\mathfrak{o}_F$ の素イデアルとする. このとき,

(I) $2 \mid a_{\mathfrak{p}}$ となるための必要十分条件は, $\mathfrak{p}$ は $F/\mathbb{Q}$ で惰性するか, または分解して, かつ $m = -1$ (resp. $= -3$) のとき合同条件 $p \equiv 1 \mod 8$ (resp. $p \equiv 1 \mod 12$) をみたすことである.

(II) $2 \mid a_{\mathfrak{p}}$ のとき, $K^{\mathfrak{p}}/F$ はいつも NIB をもつ.

命題 36. $\mathfrak{p}$ をある奇素数の上にある $\mathfrak{o}_F$ の素イデアルとし，$\mathfrak{p}$ は $F/\mathbb{Q}$ で惰性すると仮定とする．このとき，$2 \mid a_{\mathfrak{p}}$ かつ $K^{\mathfrak{p}}/F$ は NIB をもつ．

定理 37. $m = -2$ のとき，$F/\mathbb{Q}$ で完全分解する $\mathfrak{o}_F$ の素イデアル $\mathfrak{p}$ が無限個存在して，$2 \mid a_{\mathfrak{p}}$ かつ $K^{\mathfrak{p}}/F$ は NIB をもたない．$m = -\ell$, ℓ : 素数, $\ell \equiv 3 \mod 4$ のときは，次のことを仮定すると同じ主張が成り立つ:

$$p_0 \equiv 1 \mod 4,\ \ell > \frac{p_0 - 1}{4},\ \left(\frac{\ell}{p_0}\right) = 1 \tag{2}$$

をみたす素数 p_0 がある．ここで，第 3 番目の式の左辺は平方剰余記号である．

注意 38. $(\ell, p_0) = (11,5), (19,5), (43,13), (67,17), (163,41)$ とする．このとき，組 (ℓ, p_0) は条件 (2) をみたす．したがって，定理 37 は Gómez Ayala and Schertz [7, Satz 1] を導く．□

定理 39. $m \equiv 1 \mod 8$ と仮定する．$\mathfrak{p}$ を奇素数 p の上にある $\mathfrak{o}_F$ の素イデアルとし，$\mathfrak{p}$ は $F/\mathbb{Q}$ で完全分解すると仮定する．このとき，$2 \mid a_{\mathfrak{p}} \iff p \equiv 1 \mod 4$. さらに $2 \mid a_{\mathfrak{p}}$ のとき，$K^{\mathfrak{p}}/F$ が NIB をもつための必要十分条件は $\mathfrak{p}$ が単項になることである．したがって，$m = -7$ かつ $p \equiv 1 \mod 4$ のとき，$h_F = 1$ だから $K^{\mathfrak{p}}/F$ はいつも NIB をもつ．

References

1. J. Brinkhuis, *Unramified abelian extensions of CM-fields and their Galois module structure*, Bull. London Math. Soc. **24** (1992), 236–242.
2. ———, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), 333–347.
3. 藤崎源二郎, 代数的整数論入門 (下), 裳華房, 1975.
4. A. Fröhlich, *Stickelberger without Gauss sums*, in "Algebraic number fields", Proceedings of The Durham Symposium 1975, Academic Press London, 1977, 589–607.
5. ———, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemporary Mathematics, Volume **24**, American Mathematical Society, 1983.
6. E. J. Gómez Ayala, *Structure galoisienne et corps de classes de rayon de conducteur* 2, Acta Arith. **72** (1995), 375–383.
7. E. J. Gómez Ayala and R. Schertz, *Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Number Theory **44** (1993), 41–46.
8. C. Greither, *On normal integral bases in ray class fields over imaginary quadratic fields*, Acta Arith. **78** (1997), 315–329.
9. D. Hilbert, *Die Theorie der algebraischer Zahlkörper*, Gesam. Abhandl. I, 66–363 (Jber. Deutschen Math.-Ver.4 (1897), 175–546).
10. F. Kawamoto, *S*–整数環のアーベル拡大の normal basis について, 数理解析研究所講究録 "群スキームの変形と整数論への応用", **942** (1996), 98–111.

11. ———, *On normal bases of some ring extensions in number fields* I, Tokyo J. Math., **19** (1996), 129–146.
12. ———, *A remark on normal integral bases of ray class fields over quadratic fields*, 早稲田大学理工学総合研究センター 学術支援領域 (数理科学), 研究集会報告集 VIII 整数論, 1997, 13–21.
13. ———, *On quadratic subextensions of ray class fields of quadratic fields mod* $\mathfrak{p}$, preprint.
14. A. Srivastav and S. Venkataraman, *Unramified quadratic extensions of real quadratic fields, normal integral bases, and 2–adic L–functions*, J. Number Theory **67** (1997), 139–145.
15. L. Whashington, *Stickelberger's theorem for cyclotomic fields, in the sprit of Kummer and Thaine*, Théorie des Nombres (Quebec, 1987), de Gruyter, Berlin/New York, 1989, 990–993.